



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

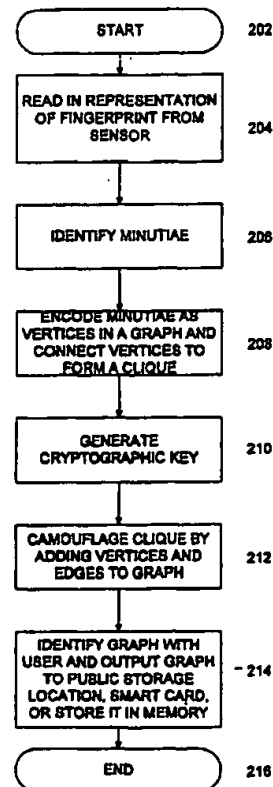
(51) International Patent Classification ⁶ : H04L 9/00	A1	(11) International Publication Number: WO 98/52317
		(43) International Publication Date: 19 November 1998 (19.11.98)
<p>(21) International Application Number: PCT/US98/09598</p> <p>(22) International Filing Date: 12 May 1998 (12.05.98)</p> <p>(30) Priority Data: 08/857,642 16 May 1997 (16.05.97) US</p> <p>(71) Applicant: VERIDICOM, INC. [US/US]; 2338 Walsh Avenue, Santa Clara, CA 95051 (US).</p> <p>(72) Inventors: PEARSON, Peter, K.; 5624 Victoria Lane, Livermore, CA 94550 (US). ROWLEY, Thomas, E.; 6366 El Paseo Drive, San Jose, CA 95120 (US). UPTON, Jimmy, R.; 2575 Katrina Way, Mountain View, CA 94040 (US).</p> <p>(74) Agent: HAYNES, Mark, A.; Wilson, Sonsini, Goodrich & Rosati, 650 Page Mill Road, Palo Alto, CA 94304-1050 (US).</p>		<p>(81) Designated States: AU, CN, JP, SG, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).</p> <p>Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i></p>

(54) Title: IDENTIFICATION AND SECURITY USING BIOMETRIC MEASUREMENTS

(57) Abstract

The present invention makes it possible for a user to have a security key (210) created from one or more biometric elements of the user, such as a fingerprint (204). For example, a biometric feature or combination of biometric features of the user can be used to create an instance of a problem which can only be solved by data inherent in the biometric feature or combination of biometric features. The user can supply the data to solve the problem by inputting, through an appropriate input device (101), an image, or other representation of the biometric elements from which the data that will solve the instance of the problem is derived. If the problem is solved, either completely or partially, using the derived data then the identity of the user can either be verified or ascertained. The solution can then be used for other purposes such as the generation of a cryptographic key (210).

ENROLLMENT SYSTEM 200



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

Identification and Security Using Biometric Measurements

Field of the Invention

The present invention relates to systems and methods for using a biometric element to create a secure identification and verification system, and more specifically to an apparatus and a method for creating a hard problem
5 which has a representation of a biometric element as its solution.

Description of Related Art

The identification or authentication of individuals is a problem that people and organizations must confront on a daily basis. A variety of systems
10 and methods are currently used to protect information and property from unauthorized access or interference. These protection systems and methods include but are not limited to conventional keys, magnetic keys, magnetic strips on cards, "smart cards," Personal Identification Numbers (PINs), and passwords.

15 Each of these systems depends on a piece of critical information or a physical access device for access to be gained. As long as the critical information or access device is retained by the rightful user, access by others will be deterred. However, if the critical information or access device is secured from the rightful owner whether by theft, fraud, duress, surveillance,
20 or consent, someone other than the rightful user could obtain access to the secure information or property.

Beyond maintaining information in a secure area through locks or password protection, it is often desirable to store or transmit information in an encrypted format so that even if the information falls into the hands of an
25 unauthorized user, it cannot be accessed without the cryptographic key. Even

while encryption allows sensitive information to be securely transmitted or stored in publicly accessible areas, encryption suffers from the same short comings of those security methods discussed above. If the cryptographic key is lost, stolen, or given away then unauthorized users may have access to the encrypted information. Since an encryption key cannot be easily memorized by the user like a PIN number or a combination to a lock, the encryption key must typically be stored in some physical medium. This leaves it vulnerable to misappropriation.

What is needed is a security method which has a key that cannot be easily misappropriated yet is convenient for the user to carry. Additionally, the lock should be difficult to open without the key, and preferably, once the lock is opened, the solution should be able to be used to generate a cryptographic key so that encrypted information can be obtained by the user.

SUMMARY OF THE INVENTION

The present invention makes it possible for a user to have a security key created from one or more biometric elements of the user, such as a fingerprint. For example, a feature or combination of features of the user can be used to create an instance of a problem which can only be solved by data inherent in the biometric feature or combination of features. The user can supply the data to solve the problem by inputting, through an appropriate input device, an image, or other representation of the biometric elements from which the data that will solve the instance of the problem is derived. The problem is solved, either completely or partially, using the derived data to verify the identity of the user, or to provide other functions.

One embodiment of the present invention works as follows. A user is enrolled through an enrollment system which is preferably in a secure location. The user biometric element that will serve as the key is sampled by an appropriate sensor. Any biometric element can be used, including a fingerprint, a palm print, a retinal scan, a picture of the user, or a combination of these elements from one or more users.

If the system is set up to use a fingerprint then the user will have the designated fingerprint scanned into the system through a fingerprint sensor. This process can be as simple as the user pressing a finger on a sensor pad. The sensor pad then inputs a representation of the fingerprint into a computer system. The representation of the fingerprint is then used to construct an instance of a problem which has data derived from the fingerprint as its solution. Preferably the instance of the problem is difficult to solve without knowledge of the fingerprint.

The instance of the problem is then associated with the identity of the user or users from which it was generated. To ensure the reliability of the system's ability to correctly identify users, it may be desirable to allow only known secure systems to generate instances of problems. The identification of an instance of a problem as corresponding to a particular user or users may be only as reliable as the process used at the enrollment system to identify the user or the security of the system used to generate the instance of the problem identified with the user.

According to one aspect of the present invention, a code or feature can be inserted into the instance of the problem in order to serve as proof that the instance of the problem was generated in a secure fashion by a secure system or that it is otherwise reliable and uncorrupted. According to another aspect of the present invention, a cryptographic key can be generated from the user's fingerprint and used to encrypt information.

Another embodiment of the present invention works as follows. A security system, access point controller, or any other device that may be used to restrict access has a user processing system in accordance with the present invention. The user processing system has a sensor that will obtain a representation of the appropriate biometric element from the user. In the example given above using a fingerprint, the sensor is a fingerprint sensor. The user presses the appropriate finger against the sensor and the sensor obtains a representation of the fingerprint. The representation of the

fingerprint is encoded into a format that can be used by the computer, and it is checked against an instance of the problem.

There are a number of ways to determine which instance or instances of the problem the representation of the fingerprint should be checked against. According to one embodiment, the user tells the processing system who the user claims to be and the processing system downloads, from a central location, a magnetic strip on a card provided by the user, or any other location, the instance of the problem identified with that person. The processing system then attempts to solve the instance of the problem using the encoded version of the user's fingerprint. According to another embodiment, the processing system can access a database of instances of the problem and determine which if any of the instances of the problem the encoded version of the user's fingerprint solves. If an instance of the problem is solved then the user's identity is determined to be the identity associated with the instance of the problem solved by the user's fingerprint.

According to another aspect of the present invention, if the user's fingerprint only partially solves the instance of the problem then this partial solution is used to reduce the work required to find a more complete partial solution. A user's fingerprint may only partially solve the instance of the problem associated with the user for any reason, including dirt masking a portion of the fingerprint or sensor, a faulty sensor, variations in how the fingerprint is read by the sensor, or the intrinsic variability of biometric elements. According to this aspect of the invention, a more complete partial solution can be found despite variability or errors in sensors or in representations of a user's fingerprint.

According to another aspect of the present invention, if the processing system solves the instance of the problem then a cryptographic key can be generated from the solution to the instance of the problem or from the user's fingerprint. This cryptographic key can be used to decrypt information meant for the user. For example, if the processing system is used to control access to a computer, the contents of the computer's hard disk can be also be encrypted.

The user gains access to the computer by pressing the appropriate finger against a sensor on the computer connected to the processing system. The processing system then also generates the cryptographic key used to decrypt the contents of the computer. For example, the cryptographic key can be used to decrypt the contents of a computer's hard disk or RAM memory.

The present invention provides a number of advantages. The user's key is the solution or a partial solution to instance of the problem. Since the user's key is constructed from the user's biometric elements, the user does not have to remember any information or carry a physical key or device, and the key cannot be easily stolen without the user's knowledge. Additionally, the user cannot easily give the key to another for unauthorized use outside the user's presence.

Another advantage of the present invention is that the instance of the problem solved by the user's key can be made as difficult as desired by the those who implement the system, making solving the problem without the key a practical impossibility. Yet another advantage of the present invention is that the degree of partial solution required by the system can be made as close to a full solution as desired by those who implement the system, making obtaining the required degree of partial solution as difficult as desired by those who implement the system.

Still another advantage of the present invention is that the system and method can be used to correct for or overcome variations in the biometric element or the representation of the biometric element by using the representation of the biometric element as an approximation to the solution to the instance of the problem. A more complete solution is then found using the approximation of the solution. A further advantage of the present system is that the solution or partial solution to the problem can itself be used to generate a cryptographic key which can be used to retrieve encrypted information of any type.

Thus, the present invention can be characterized as having two separate components. An enrollment system or method in which users are enrolled in

the security system, and a processing system or method in which a user's identity is checked by the system.

5 The system or method for enrolling a user in a biometric based verification system can be characterized as follows. A representation of a biometric element of the user is received. The representation includes a plurality of features. The plurality of features are used to produce an instance of a problem. The instance of the problem is then output to a memory location from which it can be retrieved. The instance of the problem can be stored in a centralized location available to the public, on a smart card, on the magnetic
10 strip of a credit card, or in any other suitable location.

According to one aspect of the invention the instance of the problem is produced by encoding features in the plurality of features into a plurality of encoded features. According to another aspect of the invention the step of producing the instance of the problem includes camouflaging the encoded
15 features in the instance of the problem.

According to still another aspect of the present invention, the user biometric element comprises pieces from more than one person, so that more than one person's presence is required to solve the instance of the problem.

According to yet another aspect of the invention identifying features in
20 the plurality of features in the instance of the problem requires that a hard problem be solved. The hard problem can be an NP hard problem, preferably an NP complete problem, or most preferably an exponentially hard problem to solve. A description of problem solving, complexity, and NP, NP-hard, NP-complete, and exponential time problems can be found in the book
25 "Computers and Intractability" by M.R. Garey and D.S. Johnson (1979). This book is incorporated by reference.

According to another aspect of the present invention identifying features in the plurality of features in the instance of the problem requires that a clique be found in a graph. According to still another aspect of the present
30 invention identifying features in the plurality of features in the instance of the problem requires that a subset of elements of a larger set of element be

identified wherein the elements in the subset is satisfy a predetermined condition. According to another aspect of the present invention the predetermined condition the elements of the subset must satisfy includes the condition that the sum of numerical values assigned to elements of the subset
5 is equal to a predetermined number.

According to another aspect of the present invention at least a portion of the biometric element comprises an element of a fingerprint, and the plurality features comprise an element of a plurality of minutiae.

In another embodiment of the present invention a system and method
10 for processing a user in a biometric based system includes storing in a memory information comprising an instance of a problem based on features in the plurality of features. According to another aspect of the present invention a representation of a user biometric element is received. The representation includes a plurality of user features. In another aspect of the present invention
15 it is determined if the user features in the plurality of user features partially solve the instance of the problem.

In yet another aspect of the present invention user features in the plurality of user features are used to identify a partial solution to the instance of the problem. The partial solution is then used to obtain a more complete
20 partial solution.

According to another aspect of the invention solving the instance of the problem requires that a hard problem be solved. The hard problem can be an NP hard problem, preferably an NP complete problem, or most preferably an exponentially hard problem to solve. According to yet another aspect of the
25 present problem the instance of the problem requires that a clique be identified in a graph.

According to another aspect of the present invention at least a portion of the user biometric element comprises an element of a fingerprint, and the plurality features comprise a plurality of minutiae of the fingerprint.
30 According to still another aspect of the present invention the solution or a partial solution to the problem is used to create a key. Preferably the key is a

cryptographic key. According to still another aspect of the present invention the plurality of user biometric elements are used to provide evidence that a solution or a partial solution to the instance of the problem has been found. Preferably providing evidence that a solution or a partial solution to the instance of the problem has been found is through the use of zero knowledge proof of knowledge.

BRIEF DESCRIPTION OF THE FIGURES

Figure 1 is a block diagram illustrating a system to enroll users in accordance with an aspect of the present invention.

Figure 2 is a flow chart illustrating the sequence of operations involved in enrolling a user in accordance with an aspect of the present invention.

Figure 3 is a diagram illustrating a simplified example of a fingerprint encoded as vertices in a graph, vertices forming a clique, and camouflaging of the clique with camouflage vertices and edges.

Figure 4 is a block diagram illustrating a system to process users in accordance with an aspect of the present invention.

Figure 5 is a flow chart illustrating the sequence of operations involved in processing a user in accordance with an aspect of the present invention.

Figure 6 is a flow chart illustrating the sequence of operations involved in processing a user in accordance with another embodiment of the present invention.

25

DETAILED DESCRIPTION

The following description is presented to enable a person skilled in the art to make and use the invention, and is provided in the context of a particular application and its requirements. Various modifications to the disclosed embodiments will be readily apparent to those skilled in the art, and the general principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the invention.

Thus, the present invention is not intended to be limited to the embodiments disclosed, but is to be accorded the widest scope consistent with the principles and features disclosed herein.

Figure 1 is a diagram illustrating enrollment system 100. Enrollment system 100 is preferably a secure system. Enrollment system 100 includes sensor 101 which produces a representation of a biometric element such as fingerprints, retinas, palm prints, irises, faces, signature, or any other biometric element. Although only one sensor is shown in Figure 1, any number of sensors could be connected to the system in any combination allowing biometric features from more than one portion of a single body or more than one body to be used. Sensor 101 generically represents any type of sensor including a camera, a fingerprint sensor, a laser based sensor, a pressure sensor to detect a written signature, or any other type of sensor that can be used to detect a biometric element. Examples of sensors are described in U.S. Patent Application No. 08/573,100, entitled "Fingerprint Acquisition Sensor," inventors: Alexander G. Dickinson, Ross McPherson, Sunetra Mendis and Paul C. Ross, filed 12/15/95, and U.S. Application entitled "Capacitive Fingerprint Sensor with Adjustable Gain," inventors: Alexander G. Dickinson, Ross McPherson, Sunetra Mendis and Paul C. Ross, filed 5/13/97. Both applications are commonly owned with the present application and both applications are incorporated by reference

Sensor 101 is connected to input-output line 102 which is itself connected to computer system 104. Computer system 104 includes interface 106 and processor 108 connected by interface-processor bus 110. Memory 112 is connected to processor 108 by memory-processor bus 114.

Computer system 104 generically represents any type of computer system, such as a microprocessor-based system, a mainframe system, or any other type of general or special purpose computing system which includes an interface, a processor, and a memory. Processor 108 is any type of processor such as a microprocessor, dedicated logic, a digital signal processor, a programmable gate array, a neural network, or a central processor unit

implemented in any other technology. Stored in memory 112 is representation of fingerprint 116 (or any other biometric element) and instance of problem 118.

Representation of fingerprint 116 is input to computer system 104 through input-output line 102 and stored in memory 112. As described below, representation of fingerprint 116 is encoded and camouflaged in instance of problem 118 which is stored in memory 112. Instance of problem 118 is then output to a location from which it can be retrieved for future use.

Figure 2 is a flow chart of the sequence of operations involved in enrolling a user in the enrollment system in accordance with an aspect of the present invention. Enrollment flowchart 200 starts at step 202, which is the start state. This system next proceeds to step 204.

At step 204, representation of fingerprint 116 is read from sensor 101 into computer system 104 through input-output line 102. The system then proceeds to step 206. In step 206, the minutiae present in representation of fingerprint 116 are identified. The system then proceeds to step 208.

In step 208, the minutiae identified in step 206 are encoded as vertices in a graph. The minutiae are encoded by representing them by their relative locations in representation of fingerprint 116. For purposes of illustration, a graph with 4 vertices 302 A-D is shown in Figure 3a. In Figure 3b, the vertices in the graph are then connected by edges 304 to form a clique. In one embodiment of the present invention the connections of the vertices are represented in memory 112 by an $N \times N$ matrix in which N is the number of vertices. If two vertices are connected then a "1" is placed in the array at the intersection of the row and column representing the two vertices. If there is no connection then a "0" is placed at the intersection. At this stage, since all of the vertices are connected to form the clique, the array contains only "1"s.

The system then proceeds to step 210. At step 210 a cryptographic key is generated, if desired, from the vertices of the clique. A cryptographic key can be generated, for example, as a function of the relative distances of specified vertices in the clique from a fixed point in the graph. Any method

can be used to generate a cryptographic key as long as the method reliably generates a unique key from the biometric elements of different users. A public key can then be generated and identified as associated with the graph so that encrypted information can be securely sent to the user who knows the location of the clique in the graph. In this embodiment, since the private key is generated from the clique itself, only the user who can identify the clique in the graph can decrypt the encrypted message.

The system then proceeds to step 212. At step 212, the clique is camouflaged through the addition of vertices and edges to the graph. The addition of camouflage vertices 306 and camouflage edges 308 is represented in Figure 3c. Vertices are added by generating a location for each camouflage vertex and inserting rows and columns in the array at the appropriate locations. Camouflage edges are then generated by placing either a "1" or a "0" in the newly generated rows and columns.

Care must be taken in how the camouflage vertices and edges are added to the graph in order to ensure that the camouflage vertices and edges cannot be discerned from the vertices and edges that form the clique. One way to achieve this result is to randomly place the camouflage vertices in the graph and randomly connect edges to the vertices until each vertex has approximately the same number of edges attached to it.

In order to make it difficult to find the clique camouflaged in the graph at least 5 minutiae should be encoded in the clique and at least 5 camouflage vertices should be generated. Preferably 20 or more minutiae should be encoded in the clique and also preferably 20 or more camouflage vertices should be generated. More preferably 40 or more minutiae should be encoded in the clique and also more preferably 100 or more camouflage vertices should be generated. Even more preferably 60 or more minutiae should be encoded in the clique and also even more preferably 300 or more camouflage vertices should be generated. Most preferably, 60 more minutiae should be encoded in the clique and also most preferably 500 or more camouflage vertices should be generated.

The system next proceeds to step 214. At step 214 the encoded and camouflaged instance of the problem 118 is then output from computer system 104 through input-output line 102 along with the associated public key if one was generated. Encoded and camouflaged instance of problem 118 may
5 be output to a public storage location, a smart card, or retained in memory.

Figure 4 is a diagram illustrating a system to process a user in accordance with one aspect of the present invention. System for processing a user 400 includes a sensor 401 which produces a representation of a biometric element such as images of fingerprints, retinas, palm prints, irises, faces,
10 signature, or any other biometric element. Although only one sensor is shown in Figure 4, any number of sensors could be connected to the system in any combination allowing biometric features from more than one portion of a single body or more than one body to be used. Sensor 401 generically represents any type of sensor including a camera, a fingerprint sensor, a laser
15 based sensor, a pressure sensor to detect a written signature, or any other type of sensor that can be used to detect a biometric element.

Sensor 401 is connected to input-output line 402 which is itself connected to computer system 404. Computer system includes interface 406 and processor 408 connected by interface-processor bus 410. Memory 412 is
20 connected to processor 408 by memory-processor bus 414. Stored in memory 412 is representation of user fingerprint 416 and instance of problem 418.

Computer system 404 generically represents any type of computer system, such as a microprocessor-based system, a mainframe system, or any
25 other type of general or special purpose computing system which includes an interface, a processor, and a memory. Processor 408 is any type of processor such as a microprocessor, dedicated logic, a digital signal processor, a programmable gate array, a neural network, or a central processor unit implemented in any other technology.

30 Figure 5 is a flow chart of the sequence of operations involved in processing a user in accordance with an aspect of the present invention. The

system starts at step 502, which is the start state. The system next proceeds to step 504. At step 504, representation of user fingerprint 416 is read from sensor 401 into computer system 404 through input-output line 402 and then into memory 412. Representation of fingerprint 416 can be in any form
5 desired. If it is not yet encoded so that it can be matched against an instance of a problem, then processor 408 will encode it as appropriate.

Any method of encoding can be used that will allow representation of fingerprint 416 to be matched against instance of the problem 418. For example, representation of fingerprint 416 is encoded by the same method as
10 described above for the enrollment system.

The system then proceeds to step 506. At step 506 the system determines if there is an instance of the problem 418 against which the system has not yet checked representation of user fingerprint 416. If there is an instance of a problem 418 against which the representation of user
15 fingerprint 416 has not been checked, then a new instance of the problem 418 is read into memory 412. If there is no new instance of the problem 418 to be read in, then the system goes to step 508 and reports no match.

System 400 and method 500 can be used for example, in 2 distinct types of user processing: authentication and identification. For use in
20 authentication, the instance of the problem corresponding to the person the user claims to be is input at step 510. For use in identification, a plurality of instances of a problem are input successively in step 510. The plurality of instances of the problem are preferably chosen so that the user's identity can be determined to correspond to the identity associated with one of the instances of
25 the problem in the plurality of instances of the problem. The system and method of the present invention can also be used to ensure that a user is not on a given list of users. This can be accomplished by, for example, maintaining a database of a plurality of instances of the problem associated with user's who are to be denied access by the system or method.

30 After step 510 is completed, the system then goes to step 512. At step 512 the system decides if representation of user fingerprint 416 solves

instance of problem 418. This is done by determining if the vertices in representation of user fingerprint 416 match any of the vertices in the instance of the problem loaded in step 510. If a match is found then it is determined if the matching vertices form a clique. If they do form a clique then the instance
5 of the problem is solved. If a solution or a partial solution is not found, then the system loops to step 506.

According to another aspect of the present invention the system and method can be used to correct for any variability in a representation of a biometric element from the representation used to create the instance of the
10 problem. This is true whether the origin of the variations is the biometric element itself, a sensor, or any other source or combination of sources. Correction for variations can be accomplished, for example, as follows in the case in which the system or method uses a fingerprint as the biometric element. At step 512 when the system decides if representation of user
15 fingerprint 416 solves instance of problem 418, the system determines which vertices in representation of user fingerprint 416 match vertices in the clique in instance of problem 418. The system then uses the vertices that match to help locate more vertices in the clique in the instance of the problem. In one aspect of the present invention, the system uses other vertices in the representation of
20 user fingerprint 416 to locate more vertices in the clique in instance of problem 418. This is accomplished by determining if vertices in instance of problem 418 which are closest to unmatched vertices in representation of user fingerprint 416 are vertices in the clique in instance of problem 418. Any other technique or algorithm for matching which is commonly known in the
25 art is suitable for this purpose. If after a predetermined time or a predetermined number of vertices in instance of problem 418 have been checked and no further vertices in the clique are found, then the system stops looking for more vertices in the clique in instance of problem 418.

If a solution or a partial solution is found, then step 514 is executed.
30 At step 514 the user is identified as being the person associated with instance of problem 418 loaded in step in step 510. If only a partial solution is found

then this is reported. The system can be set so that either partial solutions of a predetermined completeness end the loop between steps 512 and 506, or the system continues to loop until a complete solution is found or there are no new instances of the problem to load in at step 506.

5 If a solution is found, the system can be used to allow the user access to secure information, a secure area, or use of a device such as a computer or a cellular phone. According to another aspect of the present invention, when the solution is found, the system can attempt to prove to other systems or devices that it has found the solution. This can be achieved by releasing information
10 that only one in possession of the answer would know. More preferable, proof of knowledge of the answer is achieved through the release by system 400 of as little of the answer as is possible consistent with practical constraint such as time required to provide adequate proof and system data rates. Most preferably, the proof of knowledge of the answer by system 400 is
15 accomplished using a zero knowledge proof of knowledge. A description of proofs of knowledge and zero knowledge proofs of knowledge can be found in "Applied Cryptology" by Bruce Schneier. This book is incorporated by reference.

 After step 514, the system then proceeds to step 516. At step 516, if it
20 is desired, a private key is generated from the solution to the instance of the problem and can be used to decrypt information encrypted using the public key generated during the enrollment process. The key can be used to decrypt information stored on a computer. The system then goes to step 518 and ends.

 Figure 6 is a flow chart of the sequence of operations involved in
25 processing a user in accordance with another embodiment of the present invention. The system starts at step 602, which is the start state. The system next proceeds to step 604. In step 604 the system reads into memory 412 representation of user fingerprint 416. Representation of fingerprint 416 can be in any form desired. If it is not yet encoded so that it can be matched
30 against an instance of a problem, then processor 408 will encode it as appropriate.

The system then proceeds to step 606. At step 606 the system attempts to prove it has the answer to the instance of the problem associated with the user. As described above, this can be accomplished in a number of ways, including the use of a zero knowledge proof of knowledge. System 400 will
5 communicate through input-output port 402 with a location that stores the instance of the problem the user's representation of a fingerprint is claimed to solve. In this embodiment, system 400 need not store instance of problem 418 in memory 412. If system 400 successfully provides enough evidence that the user's biometric element solves the instance of the problem, then the user is
10 identified as the user associated with the instance of the problem solved and access to the appropriate information or property is allowed. If enough evidence is not provided the identification fails and access is denied.

The system next proceeds to step 608 where, if the problem was solved, a cryptographic key is generated, if desired, from the solution to the
15 problem. This key can be used as described above. The system then proceeds to step 610 and ends.

The foregoing description of embodiments of the present invention are presented for the purposes of illustration and description only. They are not intended to be exhaustive or to limit the invention to the forms disclosed.
20 Many modifications and variations will be apparent to practitioners skilled in the art. It is intended that the scope of the invention be defined by the following claims and their equivalents. What is claimed is:

CLAIMS

1. A method for enrolling a user in a biometric based verification system,
comprising the steps of:
 - 5 receiving from a sensor a representation of a biometric element of the user, the representation including a plurality of features;
 - producing an instance of a problem using features in the plurality of features; and
 - outputting the instance of the problem to a memory from which it can
10 be retrieved.
2. The method of claim 1 wherein the step of producing an instance of the problem includes:
 - 15 encoding features in the plurality of features into a plurality of encoded features.
3. The method of claim 2 wherein the step of producing an instance of the problem includes:
 - 20 camouflaging the encoded features in the instance of the problem.
4. The method of claim 1 wherein:
 - the instance of the problem is associated with the user.
5. The method of claim 4, wherein:
 - 25 a data structure is created that identifies the instance of the problem with the user.
6. The method of claim 1, wherein:
 - 30 a key is generated using features in the plurality of features.
7. The method of claim 6, wherein:

the key is a cryptographic key.

8. The method of claim 1, wherein:
identifying features in the plurality of features in the instance of the
5 problem requires that an NP-hard problem be solved.
9. The method of claim 1, wherein:
identifying features in the plurality of features in the instance of the
problem requires that an NP-complete problem be solved.
10
10. The method of claim 1, wherein:
identifying features in the plurality of features in the instance of the
problem requires that an exponentially hard problem be solved.
11. The method of claim 1, wherein:
identifying features in the plurality of features in the instance of the
15 problem comprises identifying a subset of elements in a larger set of elements;
wherein the subset of elements satisfies a predetermined condition.
12. The method of claim 11, wherein:
identifying the subset of elements in the larger set of elements
20 comprises identifying features in the plurality of features that comprise the
subset of elements in the larger set of elements.
13. The method of claim 12, wherein:
the predetermined condition is a numerical sum.
25
14. The method of claim 12, wherein:
the predetermined condition is a clique in a graph.
30
15. The method of claim 1, wherein:

identifying features in the plurality of features in the instance of the problem requires that a clique be found in a graph.

5 16. The method of claim 1, wherein:
 the biometric element comprises biometric elements from one or more people.

10 17. The method of claim 1, wherein:
 the biometric element comprises an element of a fingerprint.

18. The method of claim 1, wherein:
 the biometric element comprises an element of a palm print.

15 19. The method of claim 1, wherein:
 the biometric element comprises an element of a plurality of fingerprints.

20 20. The method of claim 1, wherein:
 the biometric element comprises an element of an iris.

21. The method of claim 1, wherein:
 the biometric element comprises an element of a retina.

25 22. The method of claim 17, wherein:
 the plurality of features comprises an element of a plurality of minutiae.

30 23. The method of claim 2, wherein encoding the features in the plurality of features includes:
 representing features in the plurality of features as vertices in a plurality of vertices in a graph.

24. The method of claim 19, wherein encoding the features in the plurality of features includes:
connecting vertices in the plurality of vertices with edges in a plurality of edges.
25. The method of claim 24, wherein:
vertices in the plurality of vertices and edges in the plurality of edges form a clique.
26. The method of claim 25, wherein camouflaging the encoded features includes the step of:
generating camouflage vertices in a plurality of camouflage vertices.
27. The method of claim 26, wherein camouflaging the encoded features includes the step of:
generating camouflage edges in a plurality of camouflage edges.
28. The method of claim 27, wherein:
camouflage edges in the plurality of camouflage edges are connected to camouflage vertices in the plurality of camouflage vertices.
29. The method of claim 28, wherein:
camouflage edges in the plurality of camouflage edges are connected to vertices in the plurality of vertices.
30. The method of claim 29, wherein:
the instance of the problem comprises finding the clique in a graph.
31. A method for processing a user in a biometric based system comprising the steps of:

storing information comprising an instance of a problem based on features in a plurality of features of a biometric element; and attempting to solve the instance of the problem.

- 5 32. The method of claim 31, wherein the step of attempting to solve the instance of the problem includes:
 receiving a representation of a user biometric element from a sensor, the representation including a plurality of user features.
- 10 33. The method of claim 32, wherein the step of attempting to solve the instance of the problem includes:
 determining if user features in the plurality of user features partially solve the instance of the problem.
- 15 34. The method of claim 31, wherein:
 a result of attempting to solve the instance of the problem includes a partial solution to the instance of the problem.
- 20 35. The method of claim 31, wherein:
 if the instance of the problem is at least partially solved then the user is identified as being a user associated with the instance of the problem.
- 25 36. The method of claim 31, wherein:
 the instance of the problem comprises an NP-hard problem.
- 30 37. The method of claim 31, wherein:
 the instance of the problem comprises an NP-complete problem.
38. The method of claim 31, wherein:
 the instance of the problem comprises an exponentially hard problem.

39. The method of claim 31, wherein:
the instance of the problem comprises identifying a subset of elements
in a larger set of elements; wherein
the subset of elements satisfies a predetermined condition.
- 5
40. The method of claim 39, wherein:
identifying the subset of elements in the larger set of elements
comprises identifying features in the plurality of features that comprise the
subset of elements in the larger set of elements.
- 10
41. The method of claim 40, wherein:
the predetermined condition is a numerical sum.
42. The method of claim 40, wherein:
15 the predetermined condition is a clique in a graph.
43. The method of claim 31, wherein:
the instance of the problem comprises identifying a clique in a graph.
- 20
44. The method of claim 32, wherein:
the user biometric element comprises pieces from more than one
person.
- 25
45. The method of claim 32, wherein:
the user biometric element comprises an element of a fingerprint.
46. The method of claim 32, wherein:
the user biometric element comprises an element of a palm print.
- 30
47. The method of claim 32, wherein:

the user biometric element comprises an element of a plurality of fingerprints.

5 48. The method of claim 32, wherein:
the user biometric element comprises an element of an iris.

49. The method of claim 32, wherein:
the user biometric element comprises an element of a retina.

10 50. The method of claim 32, wherein:
the plurality of features comprises an element of a plurality of minutiae.

15 51. The method of claim 43, wherein determining if features in the
plurality of features match enrollment features in the plurality of enrollment
features includes:
encoding features in the plurality of features as vertices in a plurality of
vertices.

20 52. The method of claim 51, wherein determining if features in the
plurality of features match enrollment features in the plurality of enrollment
features includes:
determining if vertices in the plurality of vertices can be mapped to a
clique in the instance of the enrollment problem.

25 53. The method of claim 31, wherein:
if a solution to the instance of the problem can be found then the
solution to the instance of problem is found.

30 54. The method of claim 53, wherein:
the solution is used to create a key.

55. The method of claim 54, wherein:
the key is a cryptographic key.
56. The method of claim 31, wherein:
5 features in the plurality of features are used to create a key.
57. The method of claim 56, wherein:
the key is a cryptographic key.
- 10 58. The method of claim 34, including the step of:
providing evidence that the partial solution to the instance of the
problem has been found.
- 15 59. The method of claim 58, wherein the step of providing evidence that a
partial solution to the instance of the problem has been found includes the step
of:
using a zero knowledge proof of knowledge.
- 20 60. A system for enrolling a user in a biometric based verification system,
comprising:
a processor that reads a representation of a biometric element of the
user, the representation including a plurality of features, and produces an
instance of a problem using features in the plurality of features.
- 25 61. A system for enrolling a user in a biometric based verification system,
comprising:
a memory that stores a representation of a biometric element of the
user, the representation including a plurality of features; and
a processor that reads the representation and produces an instance of a
30 problem using features in the plurality of features.

62. A system for enrolling a user in a biometric based verification system, comprising:
- a sensor that produces a representation of a biometric element and stores the representation in a memory;
 - 5 a processor that identifies a plurality of features of the biometric element and produces an instance of a problem using features in the plurality of features; and
 - a resource that stores the instance of the problem in the memory.
- 10 63. The system of claim 62, wherein:
- the processor encodes features in the plurality of features into encoded features.
64. The system of claim 63, wherein the processor that identifies the plurality of features includes:
- 15 a resource that camouflages the encoded features in the instance of the problem
65. The system of claim 62, wherein:
- 20 the instance of the problem is associated with the user.
66. The system of claim 65, wherein:
- a data structure is created that identifies the instance of the problem with the user.
- 25 67. the system of claim 62, wherein:
- a key is generated using features in the plurality of features.
68. the system of claim 67, wherein:
- 30 the key is a cryptographic key.

69. The system of claim 62, wherein:
identifying features in the plurality of features in the instance of the
problem requires that an NP-hard problem be solved.
- 5 70. The system of claim 62, wherein:
identifying features in the plurality of features in the instance of the
problem requires that an NP-complete problem be solved.
- 10 71. The system of claim 62, wherein:
identifying features in the plurality of features in the instance of the
problem requires that an exponentially hard problem be solved.
- 15 72. The system of claim 62, wherein:
identifying features in the plurality of features in the instance of the
problem comprises identifying a subset of elements in a larger set of elements;
wherein the subset of elements satisfies a predetermined condition.
- 20 73. The system of claim 72, wherein:
identifying the subset of elements in the larger set of elements
comprises identifying features in the plurality of features that comprise the
subset of elements in the larger set of elements.
- 25 74. The system of claim 73, wherein:
the predetermined condition is a numerical sum.
- 30 75. The system of claim 73, wherein:
the predetermined condition is a clique in a graph.
76. The system of claim 62, wherein:
identifying features in the plurality of features in the instance of the
problem requires that a clique be found in a graph.

77. The system of claim 62, wherein:
the user biometric element comprises pieces from more than one
person.
- 5 78. The system of claim 62, wherein:
the biometric element comprises an element of a fingerprint.
79. The system of claim 62, wherein:
the biometric element comprises an element of a palm print.
- 10 80. The system of claim 62, wherein:
the biometric element comprises an element of a plurality of
fingerprints.
- 15 81. The system of claim 62, wherein:
the biometric element comprises an element of an iris.
82. The system of claim 62, wherein:
the biometric element comprises an element of a retina.
- 20 83. The system of claim 62, wherein:
features in the plurality of features comprises minutiae in a plurality of
minutiae.
- 25 84. The system of claim 64, wherein:
a resource represents encoded features in the plurality of encoded
features as vertices in a plurality of vertices.
85. The system of claim 84, wherein:
30 a resource connects vertices in the plurality of vertices with edges in a
plurality of edges.

86. The system of claim 85, wherein:
vertices in the plurality of vertices and edges in the plurality of edges
form a clique.
- 5 87. The system of claim 86, wherein the resource that camouflages the
encoded vertices includes:
a resource that generates camouflage vertices in a plurality of
camouflage vertices.
- 10 88. The system of claim 87, wherein the resource that camouflages the
encoded vertices includes:
a resource that generates camouflage edges in a plurality of camouflage
edges.
- 15 89. The system of claim 88, wherein:
camouflage edges in the plurality of camouflage edges are connected to
camouflage vertices in the plurality of camouflage vertices.
- 20 90. The system of claim 89, where:
camouflage edges in the plurality of camouflage edges are
connected to vertices in the plurality of vertices.
- 25 91. The system of claim 90, wherein:
the instance of the problem comprises finding the clique in a graph.
92. A system for processing a user in a biometric based system comprising:
a resource that stores a data set in memory, the data set comprising an
instance of a problem that is based on features in a plurality of features of a
biometric element; and
30 a processor that attempts to solve the instance of the problem.

93. The system of claim 92, wherein the system includes:
a resource that receives a representation of a user biometric element
from a sensor and stores the representation in the memory;
wherein the processor user the representation to attempt to solve the
instance of the problem.
94. The system of claim 93, wherein:
the representation of the user biometric element comprises a plurality
of user features.
95. The system of claim 94, wherein:
a result from the resource that attempt to partially solve the instance of
the problem includes a partial solution to the instance of the problem
96. The system of claim 92, wherein:
if the problem is at least partially solved then the user is identified as
being a user associated with the instance of the problem.
97. The system of claim 92, wherein:
the instance of the problem comprises an NP-hard problem.
98. The system of claim 92, wherein:
the instance of the problem comprises an NP-complete problem.
99. The system of claim 92, wherein:
the instance of the problem comprises an exponentially hard problem.
100. The system of claim 92, wherein:
the instance of the problem comprises identifying features in the
plurality of features that comprise a subset of elements in a larger set of
elements; wherein

the subset of elements satisfies a predetermined condition.

101. The system of claim 100, wherein:

5 identifying the subset of elements in the larger set of elements
comprises identifying features in the plurality of features that comprise the
subset of elements in the larger set of elements.

102. The system of claim 101, wherein:

10 the predetermined condition is a numerical sum.

103. The system of claim 101, wherein:

the predetermined condition is a clique in a graph.

104. The system of claim 92, wherein:

15 the problem comprises identifying a clique in a graph.

105. The system of claim 93, wherein:

20 the user biometric element comprises pieces from more than one
person.

106. The system of claim 93, wherein:

the user biometric element comprises an element of a fingerprint.

107. The system of claim 93, wherein:

25 the user biometric element comprises an element of a palm print.

108. The system of claim 93, wherein:

30 the user biometric element comprises an element of a plurality of
fingerprints.

109. The system of claim 93, wherein:

the user biometric element comprises an element of an iris.

110. The system of claim 93, wherein:

the user biometric element comprises an element of a retina.

5

111. The system of claim 92, wherein:

the plurality of features comprises an element of a plurality of minutiae.

10

112. The system of claim 94, wherein:

the processor includes a resource that encodes user features in the plurality of user features as user vertices in a plurality of user vertices.

15

113. The system of claim 112, wherein:

the processor includes a resource that determines if user vertices in the plurality of user vertices can be at least partially mapped onto a clique that partially solves the instance of the problem.

20

114. The system of claim 113, wherein:

if the processor can find a partial solution to the instance of the problem then the partial solution is found.

25

115. The system of claim 114, wherein:

a resource uses the partial solution to create a key.

116. The system of claim 115, wherein:

the key is a cryptographic key.

30

117. The system of claim 92, wherein:

a resource uses user features in the plurality of user features to create a key.

118. The system of claim 117, wherein:
the key is a cryptographic key.

119. The system of claim 114, wherein:
5 a resource provides a plurality of evidence that the partial solution to
the instance of the problem has been found.

120. The system of claim 119, wherein:
evidence in the plurality of evidence is provided using a zero
10 knowledge proof of knowledge.

121. A system for processing a user in a biometric based system comprising:
a resource that receives a representation of a user biometric element
from a sensor and stores the representation in the memory, the representation
15 containing features in a plurality of features of a biometric element; and
a resource that provides a plurality evidence that a partial solution to an
instance of a problem has been found based on features in the plurality of
features.

122. The system of claim 121, wherein:
evidence in the plurality of evidence is provided using a zero
20 knowledge proof of knowledge.

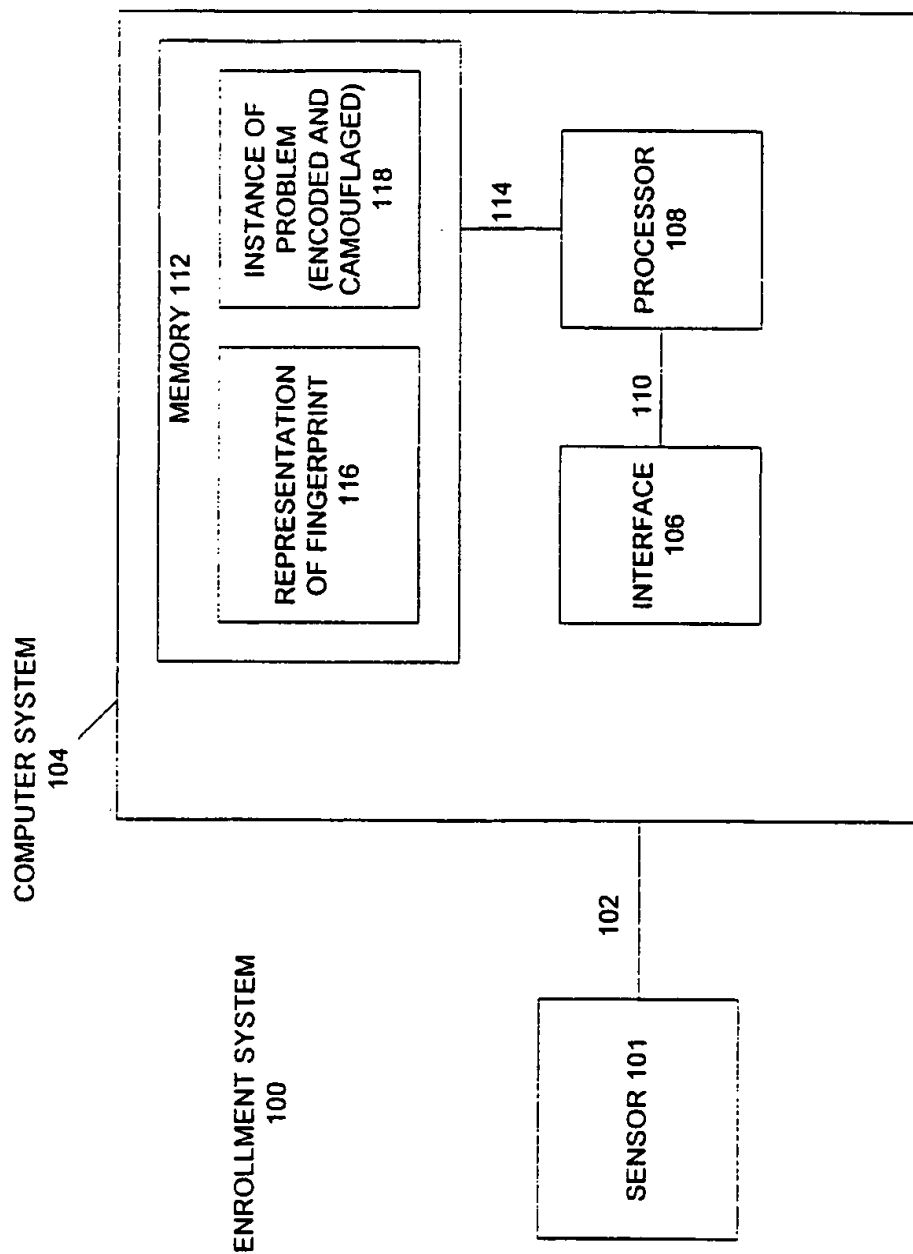


FIGURE 1

ENROLLMENT SYSTEM 200

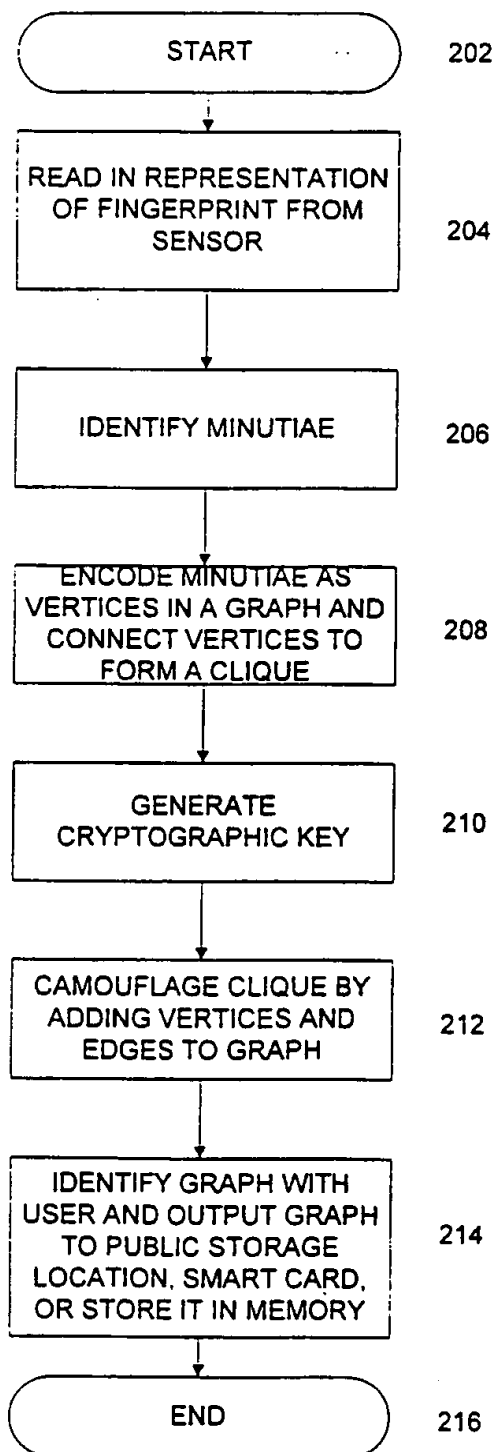


FIGURE 2

3/6

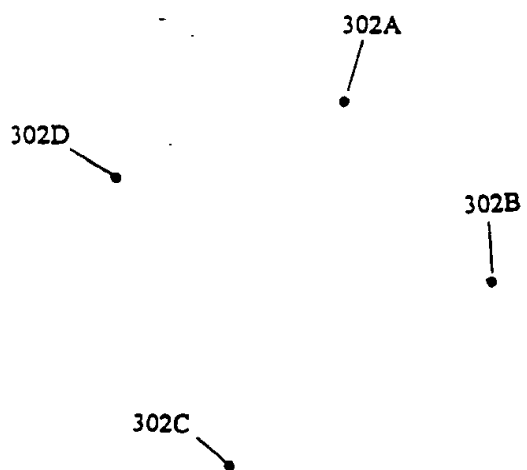


FIGURE 3a

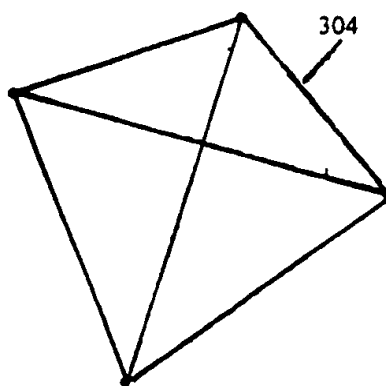


FIGURE 3b

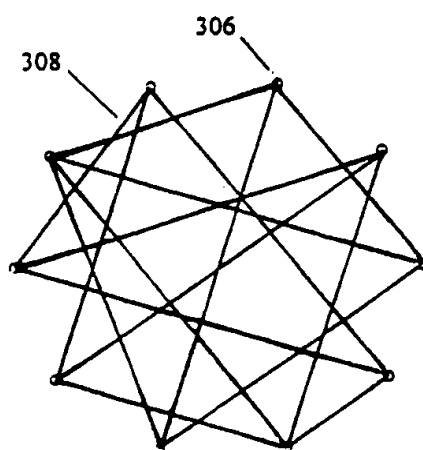


FIGURE 3c

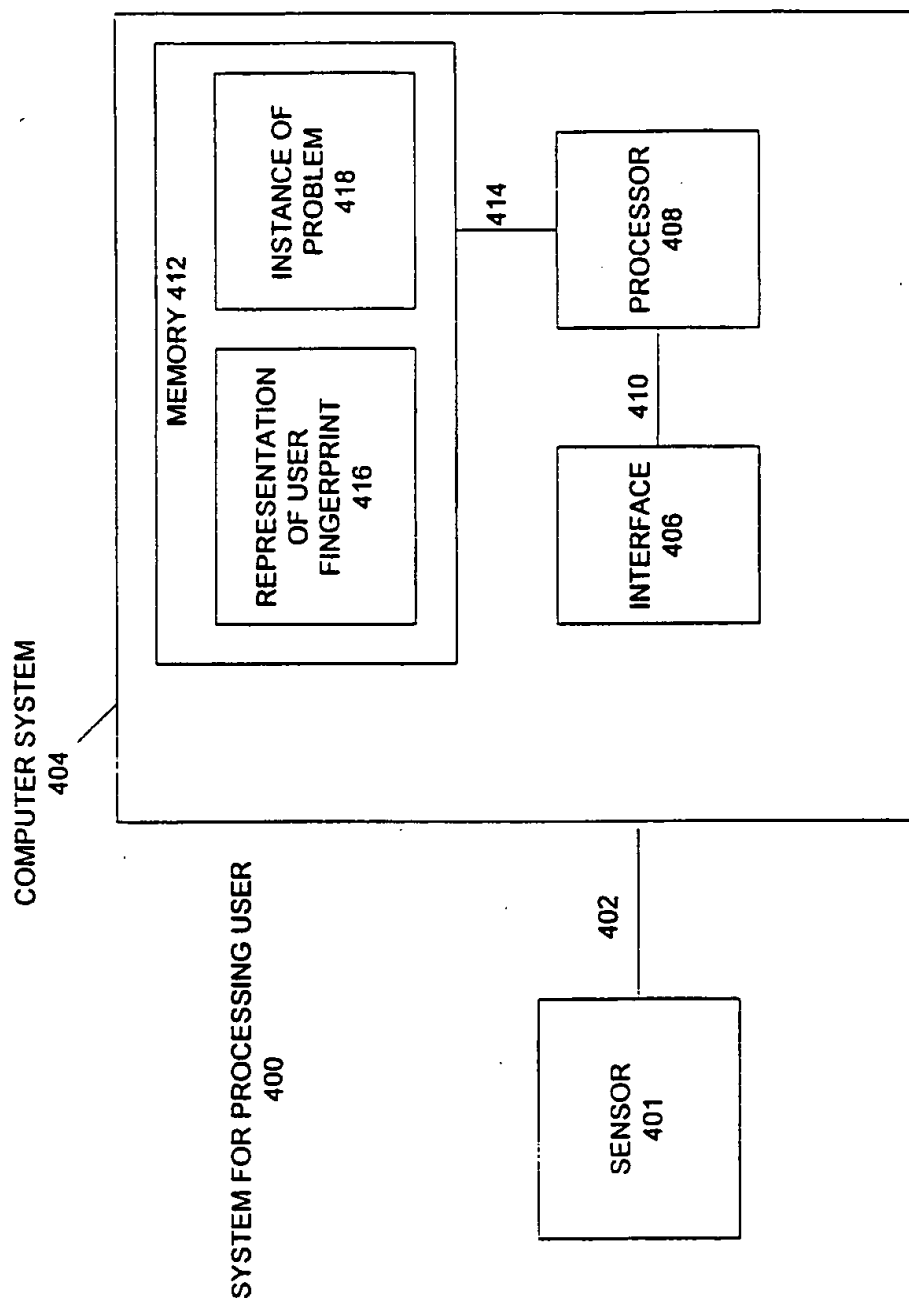


FIGURE 4

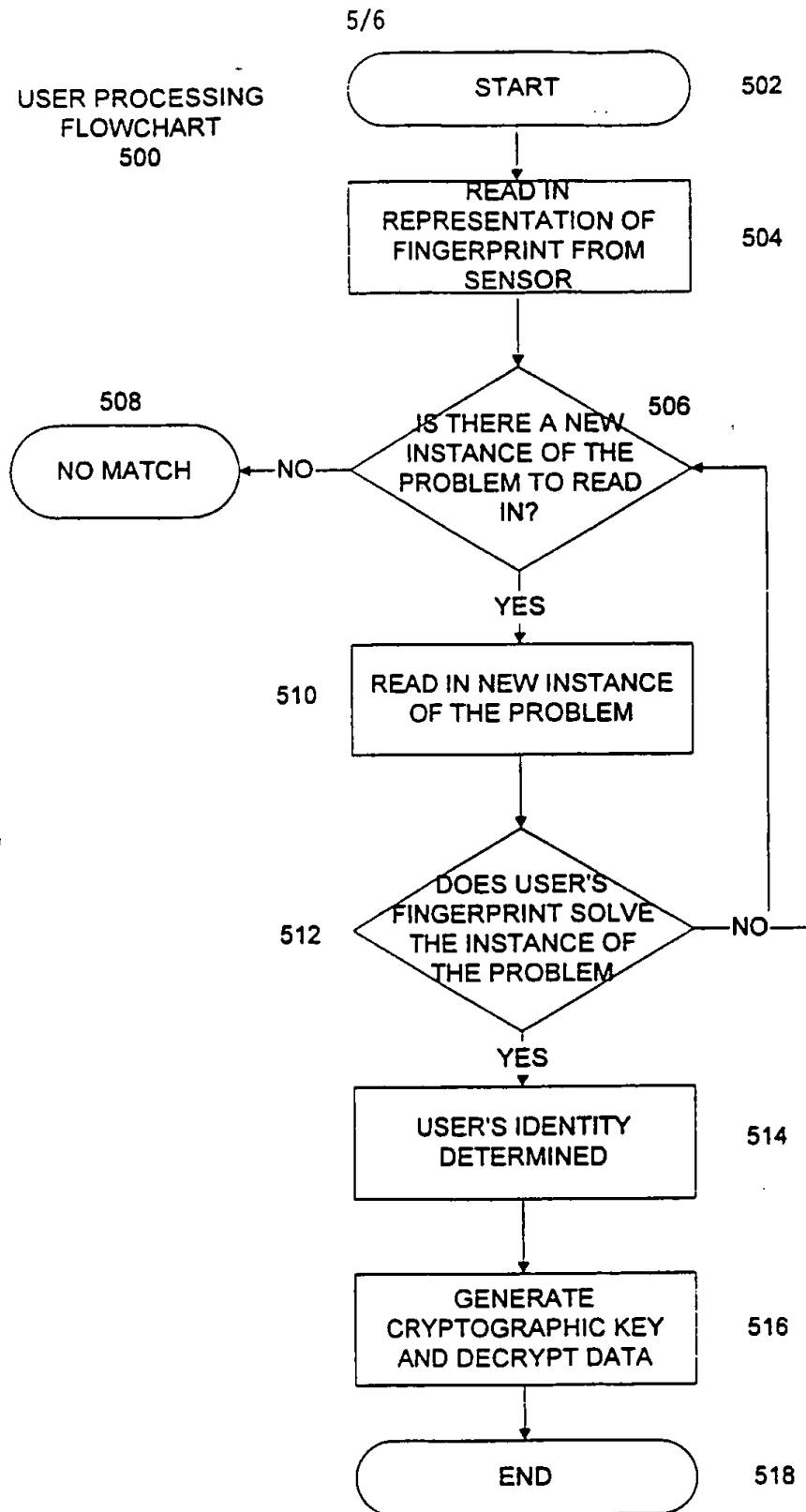


FIGURE 5

USER PROCESSING FLOWCHART USING PROOF OF KNOWLEDGE
600

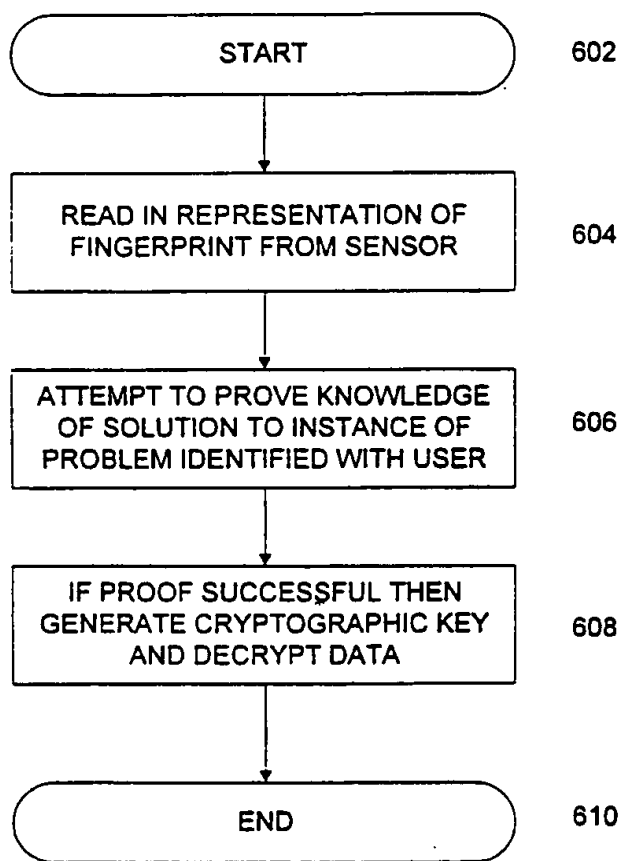
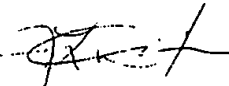


FIGURE 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US98/09598

A. CLASSIFICATION OF SUBJECT MATTER		
IPC(6) :H04 L 9/00 US CL :380/23 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) U.S. : 380/23 380/30		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, 4,993,068 (PIONSENKA ET AL) 12 February 1991 See Fig. 1.	1-122
Y	US, 5,541,994 (TOMKO ET AL) 30 July 1996 See Fig. 2.	1-122
Y, P	US, 5,680,460 (TOMKO ET AL) 21 October 1997 See Fig. 2.	1-122
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* *A* *E* *L* *O* *P*	Special categories of cited documents: document defining the general state of the art which is not considered to be of particular relevance earlier document published on or after the international filing date document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) document referring to an oral disclosure, use, exhibition or other means document published prior to the international filing date but later than the priority date claimed	*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art *&* document member of the same patent family
Date of the actual completion of the international search 01 JULY 1998		Date of mailing of the international search report 28 SEP 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230		Authorized officer SALVATORE CANGIALOSI  Telephone No. (703) 305-1837